2. Hack, laugh, uncover, win!

Hacking our ping tool? Let's uncover secrets and flag victory!

Here's another step in our cyber adventure! Let's move forward and dive into the challenge ahead.

Despite our efforts, vulnerabilities may still lurk. Your mission? To test the tool's defenses, exploit its weaknesses, and uncover hidden flags.

Challenge

This challenge involves a tool that pings given hosts. The goal is to exploit a command injection vulnerability in the user-supplied domain. However, the application has blacklisted many commands and special characters, including spaces and slashes. To bypass the filter, you'll need to construct the path for the flag using the `HOME` environment variable.

- Target Application: Asset Discovery tool
- Initial Endpoint: `http://web0x09.hbtn/app3/`

```
Useful instructions:
1. Log into Asset Discovery tool.
2. ping is vulnerable.
3. We can try and give it an input (google.com for example).
4. To exploit this vulnerability, we need to use Bypass space, Bypass
command check.
5. The flag is in /var/2-flag.txt
6. Path crafted with HOME bypasses filter.
7. Player supplied with source code.
```

domain=google.com;execIFSbash{IFS}-cIFS'cat{IFS}$HOME:0:1$var{HOME:0:1}2-flag.txt'